Comment sortir des discours génériques et mettre en place des solutions concrètes ?

Jean LANGLOIS-BERTHELOT & Christophe GAIE

La souveraineté technologique s'est imposée comme un point de passage obligé du débat stratégique européen. Elle irrigue les politiques industrielles, structure les discours publics et s'invite dans les écosystèmes d'innovation. Pourtant, derrière cette omniprésence, une ambiguïté persiste. La souveraineté technologique est souvent mobilisée comme un cadre général, parfois comme un mot d'ordre, rarement comme un objet d'analyse rigoureux. Or, la réalité est moins conceptuelle que matérielle. Elle se lit dans les parts de marché, les dépendances technologiques, les architectures numériques et les capacités de substitution. Le déplacement en cours est net. Comme le met en avant le *policy paper* SKEMA Publika, *Intelligence artificielle et souveraineté européenne*[1], la souveraineté ne se joue plus seulement dans la capacité à produire, mais dans la capacité à maîtriser des systèmes complexes dont les briques sont distribuées, imbriquées et, pour une large part, hors de contrôle européen. Ce basculement s'observe aussi dans le cyber, qui constitue aujourd'hui le point de convergence des dépendances technologiques.

A. LE CYBER, CŒUR INVISIBLE DE LA DEPENDANCE

Aujourd'hui, l'économie européenne repose, pour une large part, sur une infrastructure numérique pour laquelle elle ne maîtrise que partiellement le socle technologique. En effet, la part du marché du cloud européen est détenue aux deux tiers par les trois grands acteurs américains que sont

[1] Dibiaggio, L. Nesta, L. Vannuccini, S. Vidal, F. Scull, S. (2025). Intelligence Artificielle et souveraineté européenne. SKEMA Publika. https://publika.skema.edu/fr/intelligence-artificielle-et-souverainete-europeenne/

Amazon (avec AWS), Microsoft (avec Azure) et Google (avec GCP)[2]. Une part substantielle des outils de cybersécurité déployés au sein des grandes organisations provient également d'éditeurs non européens comme Palo Alto Networks ou CrowdStrike. De plus, les systèmes d'exploitation, les environnements de virtualisation, les outils de supervision ou encore les briques d'identité numérique sont fréquemment mises en œuvre par des acteurs hors UE. Nous pouvons citer comme exemples les géants du numérique Microsoft et Google.

Cette situation produit un effet spécifique : la dépendance ne se voit pas toujours. En d'autres termes, elle est insidieuse dans la mesure où elle ne se situe pas nécessairement dans l'application finale, mais dans les couches intermédiaires, celles qui orchestrent, administrent et sécurisent les systèmes[3]. Une organisation peut localiser ses données sur le territoire européen et en même temps rester dépendante d'architectures qu'elle ne contrôle pas. Concrètement une organisation peut sécuriser ses accès et dépendre d'outils dont elle ne maîtrise ni les mises à jour ni les mécanismes internes. Dans le domaine militaire l'exemple de la dépendance aux Etats-Unis avec le F-35 représente un cas typique. Un pays peut matériellement détenir un avion de chasse sans pour autant être en capacité d'accéder au contenu ou de modifier les logiciels indispensables à son fonctionnement. Ceux-ci restent, sauf disposition contractuelle spécifique, exclusivement possédés et maintenus par le fournisseur[4]. Dans ce cas, la souveraineté n'est pas pleinement assurée.

Or, c'est souvent lors d'une crise que les conséquences d'un défaut de souveraineté technologique apparaissent clairement. En effet, les attaques par ransomware qui ont touché des collectivités territoriales, des hôpitaux ou des opérateurs publics ces dernières années ont souligné cette dépendance technologique. Au-delà de vulnérabilité dans la capacité d'intrusion, les organisations on fait face à une difficulté majeure à reprendre le contrôle de leur système d'information. Du fait de l'absence de solution alternative, pour basculer leurs applications et leurs données, certains services numériques ont dû être coupés et sont restés indisponibles pendant une longue durée. Cette décision douloureuse mais nécessaire a

[2] Synergy Research Group. Q1 Cloud Spending Grows by Over $10 Billion from 2022; the Big Three Account for 65% of the Total | Synergy Research Group. https://www.srgresearch.com/articles/q1-cloud-spending-grows-by-over-10-billion-from-2022-the-big-three-account-for-65-of-the-total

[3] Bannerman, S. (2022). Platform imperialism, communications law and relational sovereignty. New Media & Society, 26(4), 1816–1833. https://doi.org/10.1177/14614448221077284

[4] Daniez, C. (2026). « Les Etats-Unis peuvent étouffer l'usage des F-35 de leurs alliés de plusieurs manières » - l'Opinion. *L'Opinion*. https://www.lopinion.fr/international/les-etats-unis-peuvent-etouffer-lusage-des-f-35-de-leurs-allies-de-plusieurs-manieres

généré des difficultés opérationnelles importantes pouvant nécessiter un retour au formulaire papier[5] ...

Par ailleurs, la vulnérabilité liée à cette dépendance latente s'est manifestée de manière spectaculaire en 2024 lors de la panne mondiale provoquée par une mise à jour défectueuse de l'éditeur américain de cybersécurité CrowdStrike[6]. Celle-ci a instantanément paralysé des millions de systèmes Windows à travers le monde, bloquant à cette occasion des aéroports, des hôpitaux et des infrastructures critiques européennes. Cet événement a démontré que la dépendance ne réside pas uniquement dans l'accès et la gestion des données, mais également dans le contrôle des flux de mise à jour des solutions de sécurité installées au cœur des systèmes informatiques.

Dans un contexte de dépendance technologique, le cyber cesse d'être une fonction de protection et devient une condition de continuité. Par conséquent, la souveraineté technologique ne peut plus être pensée sans intégrer cette dimension : qui contrôle les accès, qui administre les systèmes, qui déploie les mises à jour, qui peut, en dernier ressort, interrompre ou altérer un service. Cette dimension immatérielle de la souveraineté doit d'ailleurs être prise en compte dès l'intégration de nouvelles solutions numériques (telle l'intelligence artificielle en particulier avec l'émergence des solutions agentiques). En effet, si une organisation dépend d'une IA non souveraine pour trier ses données ou optimiser ses lignes de production, sa continuité opérationnelle est suspendue à l'éditeur du modèle[7]. C'est pourquoi le déploiement de solutions basées sur des modèles ouverts ou locaux, comme ceux de l'acteur européen Mistral AI, intégrés au sein d'infrastructures sécurisées, constitue une piste intéressante pour réduire la dépendance et améliorer la souveraineté technologique.

B. INNOVATION ET TERRITOIRES : UNE PUISSANCE FRAGMENTEE

Face à cette dépendance, l'Europe ne part pas de zéro. Elle dispose d'une base scientifique solide, représentant environ un cinquième de la production mondiale. Elle héberge des clusters technologiques performants et des écosystèmes territoriaux dynamiques. En France, des pôles (French

[5] Richy, W. (2025, February 25). Cyberattaque de l'hôpital de Versailles : plus de deux ans après, une loi en préparation. Tv78. https://tv78.com/cyberattaque-hopital-versailles-loi-cybersecurite/

[6] Rapport d'incident CrowdStrike / Agence de l'Union européenne pour la cybersécurité (ENISA), « Falcon Sensor Content Update Incident and its implications for European critical infrastructures », 2024.

[7] Commission européenne, « European AI Strategy and the role of open-source foundational models in industrial autonomy », Rapport d'orientation, 2025.

Tech Capitales) comme Rennes dans le domaine cyber, e-santé et deeptech[8], Grenoble pour les semi-conducteurs (avec STMicroelectronics et le CEA LETI)[9] ou Toulouse pour les systèmes aéronautiques et embarqués (avec Airbus et Thales Alenia Space notamment)[10] concentrent des compétences de haut niveau, associant recherche, industrie et acteurs publics. Au niveau européen nous pouvons citer l'exemple de la « Silicon Valhalla », en référence à l'écosystème de start-ups (Sana AI, Lovable etc.) extrêmement dynamique en Europe du Nord[11].

Mais cette capacité d'innovation se heurte à une limite structurelle : la difficulté à passer à l'échelle. Le nombre de start-up européennes en cybersécurité est significatif, mais très peu atteignent une taille critique comparable à leurs homologues américaines. Le financement de la *deeptech* reste inférieur, et les trajectoires industrielles sont souvent interrompues par des acquisitions ou des difficultés d'industrialisation[12]. En France, la région Bretagne a structuré le « Cyber Pôle Bretagne » (fédérant des acteurs académiques, la DGA et des industriels à Rennes) pour créer un écosystème d'innovation unique. Cependant, le constat dressé par la Cour des comptes met en lumière les difficultés chroniques de ces initiatives territoriales à transformer leurs pépites locales en champions industriels d'envergure européenne, faute de commandes publiques unifiées et de financements massifs en phase de post-amorçage[13]. Les start-up y restent hautement exposées aux rachats par des capitaux étrangers.

Cette situation crée un véritable paradoxe. L'innovation existe, mais elle ne se traduit pas systématiquement en capacité souveraine. Les territoires produisent des solutions pertinentes, testent des usages, expérimentent des

[8] Le Poool. (2026). Rapport annuel 2025 FrenchTech Rennes St Malo. https://www.lepoool.fr/LePoool_RA2025_WEB.pdf

[9] Cour des comptes. (2026, avril). Le soutien public à la filière des semi-conducteurs : Synthèse du rapport public thématique. https://www.ccomptes.fr/sites/default/files/2026-04/20260421-synthese-Soutien-filiere-des-semi-conducteurs.pdf

[10] Chambre de commerce et d'industrie Toulouse Haute-Garonne. (2023, février). Toulouse Aerospace. https://www.toulouse.cci.fr/sites/g/files/mwbcuj1576/files/2023-03/210x297-3v-TOULOUSE-AEROSPACE_fe%CC%81v2023_BD.pdf

Ministère de l'Économie et des Finances, Institut européen d'administration des affaires, & Organisation mondiale de la propriété intellectuelle. (2016). RÉINDUSTRIALISER PAR L'INNOVATION. https://www.vie-publique.fr/files/rapport/pdf/174000256.pdf

[11] SiliconValhalla. (2026). https://www.siliconvalhalla.no/about

[12] Voir le policy paper SKEMA Publika : Croissance des start-ups et PME - Pourquoi les modèles actuels atteignent leurs limites ?. https://publika.skema.edu/fr/croissance-des-start-ups-et-pme/

[13] Cour des comptes, Rapport thématique : « Le soutien public à la filière cybersécurité et le développement des écosystèmes territoriaux », Documentation française, 2025. https://www.ccomptes.fr/sites/default/files/2025-06/20250616-S2025-0602-Reponse-de-l-Etat-aux-cybermenaces-sur-systemes-d%27information-civils.pdf

technologies. Pourtant, ces innovations restent souvent confinées à des périmètres locaux ou à des phases pilotes. La diffusion vers des déploiements à grande échelle demeure limitée. La territorialisation de l'innovation constitue à la fois une force et une fragilité. Elle permet une proximité avec les besoins, une capacité d'expérimentation rapide et une spécialisation sectorielle. Mais elle génère également une fragmentation. Sans mécanisme d'intégration, les initiatives se juxtaposent sans produire d'effet de masse. Ce constat est également posé dans le *policy paper* SKEMA Publika *Intelligence Artificielle et souveraineté européenne* : au niveau européen, dans le domaine de l'IA, prédomine une logique de concurrence intra-européenne des acteurs, plutôt qu'une capacité à mobiliser des ressources complémentaires et à générer des opportunités d'innovation tout au long de la chaîne de valeur[14]. La souveraineté technologique suppose donc un changement de logique. Il ne s'agit plus seulement de soutenir l'innovation, mais d'organiser sa transformation en capacité industrielle et opérationnelle. Cela implique de connecter les territoires entre eux, d'aligner les besoins publics et privés, et de structurer des filières capables de dépasser le stade expérimental.

Cette exigence de souveraineté est d'ailleurs marquée par la matérialité physique du numérique. Plus de 95 % du trafic internet mondial passe par des câbles sous-marins[15]. Or la capacité à assurer la sécurité de ses infrastructures critiques donne la mesure de la souveraineté sur un territoire. L'exemple de Marseille est emblématique, la ville figurant maintenant parmi les dix premiers hubs mondiaux de connectivité, aux interfaces des lignes de convergence de l'Europe avec l'Afrique, le Moyen-Orient, et l'Asie. En intégrant ces emprises au sein de centres de données locaux hautement sécurisés, le territoire transforme une opportunité géographique en levier industriel et en potentiel de résilience national[16].

[14] Dibiaggio, L. Nesta, L. Vannuccini, S. Vidal, F. Scull, S. (2025). Intelligence Artificielle et souveraineté européenne. SKEMA Publika. https://publika.skema.edu/fr/intelligence-artificielle-et-souverainete-europeenne/

[15] Secrétariat général de la mer. (2022). Câbles sous-marins de communication. Dans L'économie bleue en France - Édition 2022 (pp. 397-412). Gouvernement français. https://www.info.gouv.fr/upload/media/content/0001/10/ca2753fbe56d94423b50ccf54efb30d5f4e75672.pdf

[16] Morel, C. (2020). L'État et le réseau mondial de câbles sous-marins de communication (Thèse de doctorat en droit public). Université Jean-Moulin Lyon 3. https://doi.org/10.70675/4c76d5acz07e0z4242z8830zecd385cc73ea

C. DEPENDANCES CHOISIES, SOUVERAINETE MESUREE

Le débat sur la souveraineté technologique se heurte souvent à une alternative simplificatrice : dépendance ou autonomie. Cette opposition est trompeuse car dans un système technologique globalisé, aucune économie ne peut prétendre à une autonomie complète. L'enjeu réel est celui de la dépendance choisie.

Certaines dépendances sont acceptables parce qu'elles sont maîtrisées, diversifiées ou facilement substituables. D'autres sont critiques parce qu'elles concentrent des fonctions essentielles sans alternative crédible. La distinction entre ces deux catégories doit devenir explicite et opérationnelle. Le cas des infrastructures télécoms illustre cette logique. Des acteurs comme Huawei ont proposé des solutions performantes et compétitives, accompagnées d'investissements locaux et de création d'emplois. Pourtant, plusieurs États européens ont restreint leur accès aux réseaux 5G critiques. Ce choix ne relève pas d'une opposition économique, mais d'une analyse de contrôle. Dans une infrastructure réseau, le fournisseur conserve une influence sur les mises à jour, l'architecture et certains paramètres techniques. Cette position confère un pouvoir structurel qui dépasse la simple relation commerciale.

Ce cas met en évidence un point central : l'ancrage territorial ou fiscal ne suffit pas à garantir la souveraineté. Celle-ci dépend de la capacité à contrôler, auditer, remplacer et maintenir un système en condition opérationnelle. Cette exigence de contrôle se retrouve au cœur des infrastructures immatérielles. La mise en œuvre de la doctrine de l'État français « Cloud au centre » illustre parfaitement la complexité de cette dépendance choisie. C'est l'ambition du consortium S3NS, une alliance entre Thales et Google Cloud, conçu pour répondre aux exigences de souveraineté du label SecNumCloud de l'ANSSI. L'enjeu opérationnel n'est pas ici l'autarcie technologique, mais bien la garantie de réversibilité technique et d'immunité face aux réglementations extraterritoriales telles que le *FISA* ou le *Cloud Act* américain. Cela permet aux institutions de conserver les clés de chiffrement et le contrôle opérationnel exclusif de leurs données[17].

Cette logique s'étend également à l'ensemble des technologies numériques. Le cloud, les systèmes d'identité, les logiciels critiques ou les chaînes de données doivent être évalués non seulement en termes de performance,

[17] Agence nationale de la sécurité des systèmes d'information (ANSSI). (2022). Référentiel d'exigences de sécurité pour les prestataires de services de confiance Cloud (SecNumCloud) (Version 3.2). Secrétariat général de la défense et de la sécurité nationale. https://cyber.gouv.fr/documents/388/secnumcloud-referentiel-exigences-v3.2.pdf

mais en termes de contrôle et de réversibilité. Le coût apparent d'une solution ne reflète pas son coût stratégique. Une technologie peu coûteuse peut générer une dépendance durable. Une technologie plus exigeante peut offrir une capacité de décision et de continuité. Dans ce cadre, la souveraineté technologique devient mesurable. Elle se lit dans la capacité à identifier les points critiques, à organiser des alternatives et à maintenir une continuité d'action en situation dégradée. Le cyber en constitue le révélateur, car il concentre les dépendances invisibles et les capacités de contrôle. Elle requiert de s'appuyer sur une législation bien calibrée et applicable qui joue son rôle de protection sans empêcher l'innovation.

La souveraineté technologique n'est donc ni un slogan ni une catégorie d'acteurs. Elle correspond à une transformation plus profonde de la manière dont les États et les économies appréhendent la technologie. Les données disponibles montrent une dépendance significative sur les couches numériques critiques, une capacité d'innovation réelle mais insuffisamment industrialisée, et une fragmentation territoriale qui limite l'effet d'échelle.
L'enjeu n'est pas de réduire ces constats à une opposition idéologique. Il est de les traiter comme des variables opérationnelles. La souveraineté technologique ne se décrète pas. Elle se construit dans l'articulation entre cyber, régulation, innovation et territoires, et se vérifie dans la capacité à continuer à fonctionner lorsque les conditions deviennent défavorables.
C'est à cet endroit précis que la souveraineté technologique cesse d'être un terme générique et devient un outil d'analyse qui cherche des solutions pour protéger les citoyens.